BIT Development Security Best Practices

There are practices that developers can follow throughout development to ensure application security. These practices are:

1. Code/application age (this is by far the largest security issue)
    a. The older the code/application, the more vulnerable it is.
    b. Rewriting and patching can only be done so long before the need arises to rewrite the code/pages in a newer, better version of the language.
    c. Stay mindful of the application life and when nearing the end, rewrite/eliminate the application.
2. Server side input validation. This means no JavaScript is relied on to validate your input. All validation is in code behind. Regular Expression validation (Regex) is used for this kind of validation.
    a. Input is present when required
    b. Input type is correct (string, number, etc)
    c. Input length is correct (min and max)
    d. Input format is correct
    e. Input does not contain harmful data
3. Output data is verified before display of any kind.
4. Authentication
    a. Membership providers are used instead of custom authentication
    b. Windows authentication is used when possible
    c. User login information is validated using regex and custom validation code
    d. Authentication cookies are not persisted
5. Proper error handling
    a. Try catch blocks with error handling
    b. Generic error page display when unhandled errors occur
    c. Global error handlers
6. Database protection
    a. Always refer to your connections strings in the web.config. These strings should never be hard coded.
    b. Use stored procedures to manipulate the data entered. Never hard code the SQL statements.
7. SSL or IPSec is used whenever sensitive data is being transported.
8. Understand and keep up on the risks that are out there and test your application accordingly. The most current top ten Web Application Security Risks are:
    1. Injection
    2. Cross-Site Scripting (XSS)

3. Broken Authentication and Session Management
4. Insecure Direct Object References
5. Cross-Site Request Forgery (CSRF)
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

Please keep in mind that these are not the only risks, just the top ten in a list containing many more vulnerabilities to your applications. I have provided links to each of the above risks to an explanation and prevention suggestions for all ten listed.